Statement for the Record
Robert B. Stephan

Assistant Secretary, Infrastructure Protection
National Protection and Programs Directorate
Department of Homeland Security

before the

Committee on Homeland Security
Subcommittee on Transportation Security and Infrastructure Protection
United States House of Representatives

Wednesday, May 14, 2007
311 Cannon House Office Building

"*Partnering with the Private Sector to Secure Critical Infrastructure: Has the Department of Homeland Security Abandoned the Resilience-Based Approach?"*

Thank you Chairwoman Jackson-Lee, Ranking Member Lungren, and all of the distinguished members of the Subcommittee. I appreciate the opportunity to address you on the role of the Office of Infrastructure Protection (IP) and our many partners, including the private sector, in securing and enhancing the resiliency of the Nation's critical infrastructure and key resources (CIKR). I know you have heard from my counterparts within the Department of Homeland Security on this topic, and I trust you have also received from them a resounding "No" in response to the question titling this hearing, "Has the Department of Homeland Security Abandoned the Resilience-Based Approach?" Since we have been in the process of adjusting to a major change in the American way of life since September 11, 2001, I think it is fair to say that there is resilience built into practically everything that the Department of Homeland Security (DHS) does. In fact, DHS defines resilience as "the ability to recover from, or adjust to, adversity or change." I would like to focus today on how IP works with its partners to ensure that a comprehensive, multifaceted framework exists to support the partnership dedicated to securing and enhancing the resiliency of the Nation's CIKR.

I believe that a recent article in the publication *Foreign Affairs* provides a good explanation of what we mean by "resiliency." The article stated that there are four factors, that when committed to in a sustained manner, result in resilience.[1] The first is robustness, the ability to keep operating or stay standing in the face of disaster. Second is resourcefulness, which involves skillfully managing a disaster once it unfolds. Third is rapid recovery, defined as the capacity to get things back to normal as quickly as possible after a disaster. Fourth is the statement that resilience means having the ability to absorb the new lessons that can be drawn from a catastrophe. Again, I think that DHS' efforts to date reflect these tenets, and, particularly for the

[1] "America the Resilient," Stephen E. Flynn, *Foreign Affairs*, March/April 2008.

CIKR protection mission, a sustained commitment is an absolute requirement of all members of the partnership.

The CIKR protection mission includes actions to mitigate the overall risk to assets, systems, networks, functions, or their interconnecting links resulting from exposure, injury, destruction, incapacitation, or exploitation. In the context of the National Infrastructure Protection Plan (NIPP), this includes actions to deter the threat, mitigate vulnerabilities, or minimize consequences associated with a terrorist attack or other incident. Protection can include a wide range of activities, such as hardening facilities, building resiliency and redundancy, incorporating hazard resistance into the design of a facility, initiating active or passive countermeasures, installing security systems, promoting workforce surety programs, and implementing cyber security measures, among various others. There cannot be a one-size-fits all approach to CIKR protection, and we have to devise a strategy based on a combination of considerations that reflects an understanding of vulnerabilities, interdependencies, and priorities in an all-hazards context. We view protection as an overarching risk-management strategy that fully acknowledges and supports the concept of resiliency where it offers the best solution to managing a particular risk or set of risks.

Since 9/11, significant efforts have been underway to define the scope of work required to establish the processes and mechanisms to secure and mitigate the vulnerability and ensure the functionality of CIKR across our country. The private sector has made substantial investments to boost resiliency, increase redundancy, and develop contingency plans. To support these efforts, the Department has provided nearly $14.8 billion in risk-based grant funding – with another $2.5 billion to be distributed this year – to deter threats, reduce vulnerabilities, and build resiliency.

Because the private sector owns and operates most of the Nation's critical infrastructure, DHS has successfully pursued a voluntary partnership approach, where government and the private sector work together under a common framework to set goals and priorities, identify key assets, assign roles and responsibilities, allocate resources, and measure our progress against national priorities. As important as resiliency is to a number of our critical sectors, we recognize that adopting a "one size fits all" solution could create an imbalance. The chemical, nuclear and energy sectors are prime examples of the need to balance our concerns about infrastructure restoration after an incident, with our ability to prevent the release of dangerous substances into populated areas. Preventing the loss of human life must remain our number one goal. Our efforts and accomplishments to date in partnership reflect this need for a balanced approach.

In June 2006, DHS released the NIPP, the overarching goal of which is to "Build a safer, more secure, and more *resilient* America by enhancing protection of the Nation's CIKR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency." The NIPP, which uses the word "resiliency" or a variant of it over 50 times, is the national unifying framework for understanding and managing the risk to the Nation's infrastructure through the creation of partnerships with the private sector. The 17 CI/KR Sector Specific Plans (SSPs) required under the NIPP were issued on May 21, 2007. They are the product of almost 18 months of joint effort by the CI/KR owners

and operators; State, local, territorial and tribal governments; and the federal government to identify and address sector specific risks and implement tailored risk strategies, to include tailored resiliency components.

Specifically, the NIPP provides the coordinated approach to establish national CIKR priorities, goals, and requirements so that Federal funding and resources are applied in the most effective manner to reduce vulnerabilities, deter threats, and minimize the consequences of terrorist attacks, natural disasters, and other incidents. It provides an integrated, risk-based approach to focus Federal grant assistance to State, local, and tribal entities, and to complement relevant private sector activities. It clearly identifies roles and responsibilities of all partners, and includes mechanisms to involve private sector partners in the planning process and supports collaboration among security partners to establish priorities, define requirements, share information, and maximize the use of finite resources. The NIPP serves as the unifying framework to ensure that CIKR investments are coordinated and address the highest priorities, based on risk, to achieve the homeland security mission and ensure continuity of the essential infrastructure and services that support the American government, economy, and way of life.

Achieving the NIPP goals requires meeting a series of objectives that include understanding and sharing information about terrorist threats and other hazards, building security partnerships, implementing a long-term risk management program, and maximizing the efficient use of resources. IP focuses on programs, projects, and activities that are aligned with the NIPP's objectives of Identification and Analysis, Coordination and Information Sharing, and Risk Mitigation Activities. This framework and its goals are foundational to what IP does. Every day, we work with State, local, tribal and territorial leaders and with private sector owners and operators to pursue a common goal of securing the nation's CIKR against terrorist attacks, natural disasters and other emergencies.

The NIPP provides a Sector Partnership Model through which such coordinated planning and program implementation can take place. The SSPs, developed under the umbrella of this Partnership, reflect the entire range of activities intended to accomplish the goal of security and resiliency for the sectors, and by doing so, increased preparedness. While this may sound like a relatively basic undertaking, it represents probably the first time that the government and the private sector have come together on such a large scale – literally, across every major sector of our economy – to develop a joint plan for how to protect and prepare our CIKR for natural and terrorist-related incidents. The SSPs define roles and responsibilities within each sector, catalog existing security authorities, institutionalize security partnerships already in place; and set clear goals and objectives to reduce risk, much of which also helps to prepare for disasters and set the stage for a resilient approach.

The diversity of the CIKR sectors means that different types of protection activities may be most effective for each. Certain sectors are most likely to embrace resiliency given their inherent characteristics, while others may focus more on specific types of physical protection or training or rapid response to minimize consequences; most represent a combination of various approaches. Some examples of activities focusing on resiliency include:

- In May of each year, the National Infrastructure Coordinating Center (NICC), the 24x7 watch center for coordination and communication with the CIKR sectors, disseminates a

series of documents to the CIKR sectors, which includes scenario-driven hurricane impact analyses prepared by the National Infrastructure Simulation and Analysis Center (NISAC).

- This year, NISAC has prepared 10 separate scenario analyses for simulated hurricanes making landfall in regions at high risk based on historic hurricane activity, population, and potential CIKR impacts. These pre-season analyses are intended to assist the CIKR sectors with enhanced situational awareness and response and recovery planning, based upon simulated impacts to each CIKR sector in those geographical areas, as well as a better understanding of cross sector interdependencies.

- Currently, 24 states have active Water / Wastewater Agency Response Networks (WARN) organizations, with eight more scheduled to develop WARN organizations by the end of the third quarter of 2008. The WARN system development is a direct result of the sectors third goal from the SSP "Maintain a Resilient Infrastructure."
- The Communications SSA, the National Communications System (NCS), participates in various programs that are aimed at building awareness or educating a greater community about the problem of critical infrastructure assurance and resiliency.
  - An example, the Route Diversity Forum periodically helps educate NCS member departments and agencies about improving communications resiliency.
  - To reach out to the broadcast industry, NCS works through the Federal Communications Commission (FCC), trade associations, and the FCC's Media Security and Reliability Council, which is developing best practices to ensure optimal reliability, robustness, and security of broadcast facilities. The NCS also is reaching out to other sectors with which it shares interdependencies and is assisting them in reviewing how their plans address communications interdependencies.
- As part of the Nation's electricity supply infrastructure, the nuclear sector works with regulators and other security partners to ensure that full operations are resumed as safely and quickly as possible following an incident which requires a supply reduction. Furthermore, the sector is working with its security partners to address medical radioisotope supply resiliency in the event of a disruption in the radioisotope supply chain.
  - Under the auspices of its SCC, the Nuclear Sector has completed a pilot of its proposed Prompt Notification program. The Prompt Notification capability will prepare the sector and nearby CIKR assets to defend against a geographically coordinated terrorist attack by providing a real-time mechanism for emergency communications to the Nuclear Sector, Federal entities, and critical infrastructure community partners in the vicinity of a security incident. This program will provide immediate situational and operational awareness in the event of an incident, and to enable more effective response and system restoration.
- The Commercial Facilities Sector represents one of our most diverse sectors. Yet, under the NIPP, it has come together through its SCC, in recognition of its shared risk and shared interest in protecting its assets. The participation within its council shows that there is a strong business case to be made for making investments of this kind. The companies and facilities that take steps to protect assets and plan for emergencies are

often the ones that can more quickly recover from a disruption. Joint activities for this sector include:

- The Commercial Facilities Sector Specific Agency collaboration with the Meridian Institute during their development of the Southeast Region Research Initiative), which includes the Community & Regional Resilience Initiative. These initiatives are intended to develop the processes and tools needed for communities and regions to achieve their highest measurable levels of resilience against disruptions resulting from natural and man-made disasters. Focus is placed on the ability to quickly return citizens to work, reopen schools and businesses, and restore the essential services needed for a full and swift economic and social recovery. Selected cities in the Southeast Region are participating in these initiatives. The ultimate goal of this effort is to strengthen the capability to withstand, prevent, and protect against significant multi-hazard threats so that a community, state, and region, and its private sector partners, can rapidly restore critical services, re-establish the area's economic base, and return to "normal" as quickly and effectively as possible.
- DHS conducting site assistance visits that incorporated industry feedback into a set of educational reports that owners and operators can use to identify vulnerabilities.
- DHS providing security training as well as courses on increasing terrorism awareness around commercial facilities. To date, DHS has provided a total of 408 courses for the private sector.
- Joint participation in major exercises covering terrorism, hurricane preparedness, and pandemic planning.
- Joint working group between DHS and the National Association for Stock Car Auto Racing (NASCAR) produced a planning guide for mass evacuation and a template for NASCAR facilities to use in coordinating with state and local stake holders and planning. The partnership at each of these sessions included private sector, state, local, federal partners.

- The Chemical Sector has numerous programs and initiatives which increase the Sector's resiliency. In particular the Sector's dedication to exercises enables the preparation necessary for a real incident.
  - The Chemical Sector has participated in numerous national-level exercises including Top Officials (TOPOFF) and National Level Exercise 2-08 (NLE 2-08). The Chemical Sector was active in the Cyberstorm II exercise with a dozen private sector participants. Exercises like Cyber Storm II build not only response capability, but also strong organizational and individual connections that help ensure the prevention and mitigation of attacks against our critical systems and networks.
  - Developed the Pandemic Flu Guideline for the Chemical Sector — This Annex to the Pandemic Influenza Preparedness, Response, and Recovery Guide for Critical Infrastructure and Key Resources will assist the Chemical Sector plan for a severe pandemic.
- The Dams SSA is participating in the development of a pilot study on regional disaster resilience and risk mitigation for the Columbia River Basin. This effort is conducted in collaboration with the Pacific Northwest Economic Region (PNWER), which leads the

coordination efforts. The focus of the pilot is on interdependencies and the cascading impacts associated with disruptions of dams, locks, and levees along the Columbia River Basin. In the event of natural disasters, man-made events, aging infrastructures, and sub-standard conditions, failure of these key assets could affect maritime transportation, energy, agriculture, manufacturing, the overall economy, health and human safety, and national security. The goal of this multi-year effort is to identify a holistic approach with states, localities and relevant key public and private stakeholders.

As per the National Response Framework, the Office of Infrastructure Protection has also instituted the Infrastructure Liaison (IL) to provide the private sector a vital resource during disasters, in part by enhancing the communications that are so vital to resilient systems and sectors. The IL acts as the principal advisor to the Join Field Office Coordination Group regarding all national and regional CI/KR incident-related issues and assists the Principal Federal Official in the prioritization of protection and restoration efforts. The IL coordinates CI/KR-related issues and actions with the appropriate Emergency Support Functions (ESFs) and other State and Local components represented in the JFO, providing valuable reach-back to DHS headquarters and the operational components of the National Operations Center (NOC), including the NOC Watch, the NICC, and the National Response Coordination Center (NRCC). Additionally, the IL provides impacted private sector partners with an established mechanism and process to address requests for information and assistance, either directly or via the NICC, in compliance with applicable policies and laws.

Finally, the CIKR sectors just completed participation in National Level Exercise (NLE) 2-08, which involved both a hurricane making landfall and a chemical terrorism threat. The exercise provided the opportunity for all participants to assess where they have or need redundancy for business continuity, and the ability to deal with significant potential power outages and distribution systems disruptions.

Additionally, we focus on CIKR with the activities of the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), a joint infrastructure- intelligence fusion center with the Office of Intelligence and Analysis (OI&A). HITRAC analyzes and monitors risks to U.S. CIKR, allowing IP to provide DHS decision-makers, the Federal CIKR community, owners and operators of CIKR, as well as State, local, and tribal and territorial authorities with actionable analysis and recommendations to manage risk. Analytical products are developed at the asset, sector, region, and national level and provide an understanding of the threat, CIKR vulnerabilities, the potential consequences of an attack, and the effects of risk-mitigation actions.

Again, protection can include a wide range of activities. There cannot be a one size fits all approach to CIKR protection, and we work with a variety of partners in a dynamic risk landscape to prioritize activities and devise a strategy based on a combination of considerations that reflect an understanding of vulnerabilities and interdependencies in the all hazards context. We view protection as an overarching risk management strategy that fully acknowledges and supports the concept of resiliency where it offers the best solution to managing a particular risk or set of risks. The NIPP and its supporting SSPs chart the path forward for continuous improvement of security and resiliency of our critical infrastructures, and the focused activities of IP in concert with all of our CIKR partners ensures their preparedness.

Thank you for your attention and I would be happy to answer any questions you may have at this time.